



# The private sector challenges for VFA Service Providers

*Implementing and satisfying the FIAU requirements*

**Dr. Mario Zerafa**

# VFAs and AML

1. Placement: **possibility of opening anonymous crypto accounts** provides a means for criminal groups to convert and consolidate illicit cash (custody wallet providers / exchanges).
2. Layering: Crypto provides an ideal means to **transit illicit proceeds** across borders (brokers, managers, exchanges).
3. Integration: The fact that VFAs may be used as a means of payment to **purchase an ever growing list of goods and services expands integration opportunities**.
4. Terrorism financing and sanctions evasion: The **ease of creating 'anonymous' cryptoaccounts** is ideal for persons to receive payments that might trigger red flags relating to terrorist financing or evasion of sanctions.

# VFAs and AML

1. The **need to regulate the sector** and all stakeholders within the sector is vital to ensure to mitigate risks of ML/FT.
2. **5<sup>th</sup> AMLD** only requires **custodian wallet providers and exchanges** to be subjected to AML-CFT obligations, but what about other market players?  
*A more **holistic approach** has been adopted in **Malta**.*
3. **Proper implementation** is required **to reduce ML/FT risks**.

# Main Challenges for VFA Service Providers

The main challenges being faced by VFA Service Providers:

- Business Risk Assessment;
- Customer Due Diligence;
- Ongoing Monitoring;
- Training.

# Business Risk Assessment

1. Needs to take into account the ML/FT risks arising from the **products and services** offered, the **delivery channels**, the **customers, countries, staff, third parties** and how these are to be managed through the controls to be implemented by the company.
2. An **extensive exercise** which must cover **all aspects** of the **business** and identify the necessary **controls** to be able to mitigate the risks which the company may be exposed to (including, ML,FT reputation etc).
3. Through the **inventory** provided, senior management has a **better understanding** of the risks which the activities of the company may pose and is able to manage such risks through the controls identified in the BRA.

# Business Risk Assessment

Other Risks and additional matters to be taken into account

Business Risk Assessment to take into account:

- a. Risk scenarios
- b. Likelihood / impact of scenario (inherent risk);
- c. Controls put in place to mitigate the risk and assess how effective such measures are;
- d. Determine residual risk;
- e. Assess whether it falls within your risk appetite;
- f. Determine any additional measures to be applied.

**A well documented Business Risk Assessment helps senior management in establishing the right controls and measures to mitigate ML/FT risks.**

# Customer Due Diligence

## 1. **Identifying and Verifying Client** - measures to be applied in non-face to face scenarios

may vary (to be applied on a risk sensitive basis depending on the risk):

- a. Welcome call confirming personal details and details of transactions;
- b. Requesting client to send photograph of face and identity card in the same picture;
- c. In case of fiat transactions, ensure first payment made through bank account held in the name of the customer with an EU credit institution or credit institution in a reputable jurisdiction;
- d. Certified documentation or additional documentation
- e. Other.

## 2. **Identifying and Verifying Beneficial Owner**

- a. legal entities / trusts and other structures;
- b. principal / agent relationship.

## 3. **Purpose and Intended Nature of Business Relationship:**

- a. Nature of and details concerning business / occupation / employment of customer;
- b. Other activities generating source of wealth;
- c. Expected source of funds;
- d. Anticipated level and nature of business (including expected value and frequency of transactions to be undertaken throughout the relationship).

# Customer Due Diligence

## Source of Funds

- a. Sufficiently detailed self-declarations in case of low risk clients – gaps / inconsistencies should be questioned;
- b. Source of funds information / documentation is required at inception and where unusual transactions are detected;
- c. Fiat – crypto transactions;
- d. Crypto – crypto transactions (mining / previous transactions) – screening of wallet addresses and use distributed ledger analytical tools.



# Customer Risk Assessment

1. **Online On-boarding / manual on-boarding**, depending on activities undertaken.
2. **Customer Risk Rating** based on:
  - a. Customer risk;
  - b. Geographical risk;
  - c. Delivery channel risk;
  - d. Product, Service, Transaction risk.
3. Based on the results of the Customer Risk Rating, **the appropriate controls / CDD measures** need to be applied.

# Ongoing Monitoring

1. Ensuring **documents are not expired** - risk sensitive checks / trigger events.
2. **Question data and information when inconsistencies arise** – importance of good quality data to be able to compare transactions to customer's profile and identify inconsistencies.
3. Requesting **additional documents** in case of **higher risk scenarios**.
4. **Scrutinise transactions** to ensure compatibility with customer's risk profile.
5. **Transaction Monitoring Programme** to be established:
  - a. Risk based system to monitor transactions;
  - b. Identify transactions which are unusual / suspicious;
  - c. Identify unusually large transactions / unusual patterns with no economic / visible lawful purpose.

# Ongoing Monitoring

Transaction Monitoring Programme to include the following elements:

- a. Risk based process to **identify patterns indicating suspicious behaviour** (eg. large deposits which are transferred to unrelated accounts with other unrelated wallets);
- b. Customer transaction profiling – customers conducting **activities not in line with their profile** – imposing limits.
- c. Identify customers using multiple wallets for same VFA or changes wallet for same VFA;
- d. **Comparing customer transaction profiles against transaction patterns** – changes in transactional activities;
- e. Alerts to customers identified as **high risk clients** – whether due to the type of customer or behaviour of customer.

# Ongoing Monitoring

1. Ongoing screening of **wallets** through distributed ledger analytical tools;
2. Ongoing screening of **IP addresses**;
3. Ongoing screening for **sanctions** (EU/UN/OFAC);
4. Ongoing screening for **adverse information / negative media**.

# Training

1. Training of **new employees** involved in the on-boarding of customers and in the undertaking of the relevant activity is key to identify ML/FT.
2. Employees should be trained on the:
  - a. applicable laws, regulations and guidelines issued by the FIAU;
  - b. the internal policies and procedures established by the company;
  - c. practical examples as to how to identify suspicious activity.
3. Failure to train employees could have severe consequences such as legal and regulatory sanctions as well as reputational damages.

# Remember...

1. **Proportionality** principle;
2. Well documented **procedures are to be backed up by effective systems** and **competent people** to ensure proper to ensure adequate implementation;
3. Customer due diligence is **not a tick the box exercise**;
4. It is also in **our interest** to ensure that the proper processes to identify ML/FT risks and mitigate the their occurrence;
5. **Our role is not to investigate** ML/FT but to have systems and controls in place to be able to **identify suspicious behaviour**.

# Thank you.

**Dr. Mario Zerafa**

mzerafa@ganadoadvocates.com

**[www.ganadoadvocates.com](http://www.ganadoadvocates.com)**



**Important Notice:** This presentation is for informational purposes only and does not contain or convey legal advice. The information contained in these slides should not be used or relied upon in regard to any particular facts or circumstances without first obtaining specific legal advice.

In this presentation 'GANADO Advocates' refers to the law firm Ganado & Associates, Advocates, an association established under the laws of Malta. A full list of members is available upon request at the principal office of the firm at 171, Old Bakery Street, Valletta VLT1455, Malta.